REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks.

By this amendment, claims 44 and 48 are amended. Accordingly, claims 1, 12, 14, 16, 17, 27, 28, 39, 41, 43-48, 51-57 and 65 are pending in the present application.

The amendments to claims 44 and 48 are solely directed to correction of the terminology to be used with a Markush grouping (see MPEP 2173.05 (h)). Applicants submit that the amendments to claim 44 and 48 do not raise any new issues that require further searching.

Claim Rejection Under 35 U.S.C. § 112

Claim 65 was rejected under 35 U.S.C. §112, second paragraph, as allegedly failing to comply with the written description requirement. The Office acknowledges that the applicants have disclosed replicated password servers that have the same key, but goes on to assert that this disclosure is not sufficient to describe the concept of a shared public key. The Microsoft Computer Dictionary, Fifth Edition, defines a shared resource as "Any device, data or program used by more than one device or program." A copy of the pertinent page is attached for the examiner's reference. The use of the term "shared" in the context of the present disclosure is consistent with this commonly understood meaning. Namely, a public key that is used by a plurality of computers is one that is shared by those computers.

Moreover, reference is made to paragraph 0016 of the specification, which states "Replication is the ability of multiple independent computers... to share data

and keep that data synchronized…[T]he data to be synchronized is the set of password data for an entire network of computers." (Emphasis added.)

Accordingly, it is respectfully submitted that, when the disclosure is viewed from the standpoint of a person of ordinary skill in the art, it will be understood to show that the inventors had possession of the claimed subject matter at the time the application was filed.

Claim Rejections Under 35 U.S.C. § 103

Claims 1, 12, 14, 16, 17, 27, 28, 39, 41, 43, 44, 47, 48, 51-54 and 65 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Pat. 6,795,434 ("Kumar") in view of U.S. Pat. Pub. 20030196107 ("Robertson").

Claims 55 and 57 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Kumar in view of U.S. Pat. Pub. 20030177240 ("Gulko").

Claim 56 was rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Kumar in view of Gulko and further in view of U.S. Pat. 7,039,724 ("Lavian").

Claim 1

Claim 1 recites "the backup search procedure searches for the server computer using the public key to identify the server computer." At page 4, the Office Action acknowledges that Kumar lacks a disclosure of the underlined portion of this claimed feature. Moreover, Robertson lacks this claim element for multiple reasons. First, Robertson has nothing to do with searching for a computer, and thus cannot disclose an element relating to a backup search procedure. In particular, Robertson

assumes that the computers in the IPSAN already have connectivity. Robertson, para. 0014.

Second, Robertson does not use a public key to identify a computer. Robertson first defines the unique identifier name as a "net-id" and then explains that queries are routed based on net-id: "[t]he IPSAP base server locates the IPSAP base servers of other IP networks by querying an IPSAP central server having the net-id of the destination IP network." Robertson, para. 0005. Robertson's disclosure of PGP keys is limited to traditional authentication and encryption functions. Because Robertson discloses that net-id is used to address servers, and limits PGP keys to their traditional roles, Robertson cannot suggest or disclose using a public key to identify a computer.

The Office acknowledges that Kumar lacks "the public key identifies a plurality of server computers having different network addresses." Office Action, pg. 4. The Office has asserted that Robertson discloses this feature because Robertson uses the plural term "addresses" in paragraph 0005. Applicants suggest that the appearance of the plural form "addresses" may be a typographical error as all of the other instances of "address" are in the singular.

In any event, even if the plural term was intended, it is only used in association with a single computer. Specifically, paragraph 0005 states that the central server returns the IP addresses "of the destination IPSAP base server" and the public key for that server. This phase only refers to one server. It does not disclose, nor otherwise suggest, that the returned public key identifies a plurality of computers.

Claims 17, 28 and 65 are allowable for at least the reasons above as claims 17, 28 and 65 recite similar elements.

Claims 12, 14 and 16 are allowable for at least the reasons above as claims 12, 14 and 16 depend from claim 1.

Claim 27 is allowable for at least the reasons above as claim 27 depends from claim 1.

Claims 39, 41 and 43 are allowable for at least the reasons above as claims 39, 41 and 43 depend from claim 28.

Claim 44

Claim 44 recites "searching an authentication record for the address of the server computer." The Office has asserted that Kumar's DNS lookup discloses this. (Applicants respectfully note that the Office has also admitted that Kumar lacks this. Office Action, pg. 13.) However, DNS servers differ from authentication records in two important respects. First, DNS servers are publicly available as their goal is help the public to find web servers. This public facing function of a DNS server is the opposite of authenticating, which is used to limit the number of people who can access something.

Second, the background section addresses the concern that a computer listing addresses, such as a DNS server, might fail. Specification, para. 0004. One advantage of the claimed invention is that by searching for the address through systems that are not traditionally used for address lookups, such as an authentication record, it is less likely that an error will cause system failure.

Therefore, DNS servers differ from authentication records, because DNS servers are traditionally used for internet routing.

The above discussed deficiencies of Robertson, and the inability to combine Kumar and Robertson, apply to claim 44 as well.

Claim 48 is allowable for at least the reasons above because claim 48 recites similar elements.

Claim 47 is allowable for at least the reasons above as claim 47 depends from claim 44.

Claim 51 is allowable for at least the reasons above as claim 51 depends from claim 48.

Claim 52

The Office admits that Kumar lacks "the backup search procedure including searching a configuration record of the client computer system for the network address of the server computer," as recited by claim 52.

As explained above, Robertson is unrelated to searching, and thus cannot cure any deficiencies of Kumar requiring a search. The cited section of Robertson merely states "[s]oftware on the user's computer also determines additional public information about the IP network and then acquires configuration information from the IPSAP central server and the local IPSAP base server." In contrast to searching for a network address, Robertson describes a procedure that requires already having the network address of a IPSAP server. Thus, Robertson not only lacks a search procedure, Robertson lacks searching for a network address.

Additionally, Robertson's passing reference to "configuration information" is not a "configuration record." Not only does Robertson's "configuration information" lack a network address, it does not have the possibility of storing multiple network addresses, as would be useful for searching for network addresses.

Claim 53 is allowable for at least the reasons above as claim 53 depends from claim 52.

Claim 54

The Office admits that Kumar lacks the "backup search procedure searching an authentication record for the network address of the server computer," as recited by claim 54.

As explained above, Robertson is unrelated to searching, and thus cannot cure any deficiencies of Kumar requiring a search. The cited section of Robertson merely states "Remote Authentication Dial In User Service (RADIUS) authentication (IETF RFC 2138) is used to interface the IPSAP base server with the existing authentication program." Because RADIUS is an authentication protocol, it requires that a user already be able to communicate with an authentication server, e.g., have a network address. In contrast to searching an authentication record, Robertson teaches that a server should identify the location of an authentication record - which further teaches away from either searching an authentication record or searching it for network addresses. Robertson, para. 0014.

Claim 55

Claim 55 was rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Kumar in view of U.S. Pat. Pub. 20030177240 ("Gulko").

The combination of Gulko and Kumar is inappropriate. First, the Office justified the combination by the use of public keys, but neither Gulko nor Kumar disclose public keys. Office Action, pg. 17. Second, adding a backup procedure, e.g., a backup search procedure, is the opposite of reducing computation time, which is the objective of Gulko. Office Action, pg. 17. Thus, the Office has not met its burden to show that a backup search procedure is a predictable result of an effort to reduce computation time. MPEP 2141.

As Gulko is directed to parallel processing (Gulko, title and abstract) and Kumar is directed to replicating web servers (Kumar, abstract), Gulko is in a non-analogous art with nothing to "commend[] itself to an inventor's attention in considering his or her invention as a whole." MPEP 2141.01(a).

The Office admits that Kumar lacks a "backup search procedure determining whether the server computer is running on a CPU that is the same CPU on which the client computer is running in order to determine the network address of the server computer," as recited by claim 55. Gulko also lacks this. The cited section of Gulko merely discloses that a parallelized code segment can be on a first machine or a network connected machine. In order to parallelize code, the code segments must be working in concert. In contrast, the goal of a backup procedure is that the first procedure has failed, and thus an approach that has less in common may be preferred.

Applicants note that the requirement that the code be parallelized is yet another reason that Kumar cannot be combined with Gulko, as specialized parallelized code is inappropriate for the simple tasks of Kumar, and the multitude of public users of Kumar.

Second, the entire point of distributed computing is that one need not be concerned with which computer is running a given aspect of the program. Gulko, Fig. 2A. Therefore, not only does Gulko not disclose determining if a server computer CPU is the same as a client computer CPU, Gulko teaches away from even desiring to know.

Third, as with Robertson, Gulko has nothing to do with searching, and thus cannot be used to cure deficiencies related to search procedures.

Fourth, Gulko has no disclosure of a "network address," and thus cannot disclose determining "the network address of the server computer."

Claims 56 and 57 are allowable for at least the reasons above as claims 56 and 57 depend from claim 55. Lavian is not alleged to cure the above deficiencies.

Conclusion

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: June 6, 2011

By: /David B. Orange/
David B. Orange
Registration No. 55513

Customer No. 21839
(703)836-6620